Bluetooth Packet Capture Report

12/05/2024

General Information

Capture Start Time: 2024-10-02 23:12:15
Capture End Time: 2024-10-03 07:56:50
Host Device Name: Pixel 7 Pro
Host Device MAC Address: d4:3a:2c:a9:32:4f
Host Device Vendor: Google, Inc.
Controller Devices Interacted With: 2
Total Number of Packets: 17016
HCI Command Packets: 1098
HCI Event Packets: 12563
ACL Packets: 3355

Bluetooth communication is done through a standardized protocol known as the HCI interface which allows for sending and recieving commands, events and data between hosts and controllers. We will be looking at the breakdown of these between the current host device and the controllers below.

HCI Command and Event Packet Details

Unique HCI Commands: 84
Unique HCI Events: 21
Outgoing Commands: 1098
Incoming Events: 12563

HCI Command Counts:

HCI Command	Count
LE Connection Update	188
Vendor Command 0xfd59	165
Vendor Command 0xfd57	108
Write Link Policy Settings	92
LE Set Extended Scan Enable	91
Vendor Command 0xfd5d	59
Vendor Command 0xfc57	59
Enhanced Flush	58

HCI Command	Count
Sniff Subrating	58
LE Set Random Address	48
LE Set Extended Scan Parameters	27
Sniff Mode	20
Exit Sniff Mode	18
Write Extended Inquiry Response	15
Read Remote Extended Features	4
Create Connection	4
Write Default Link Policy Settings	3
Read Local Extended Features	3
Read Remote Version Information	3
Write Link Supervision Timeout	2
Read Remote Supported Features	2
Read Clock offset	2
Change Connection Packet Type	2
Configure Data Path	2
Link Key Request Reply	2
Read Encryption Key Size	2
Read Local Name	2
Write Scan Enable	2
LE Set Extended Advertising Enable	2
Remote Name Request	1
LE Read Remote Features	1
Write Page Scan Activity	1
LE Add Device To Filter Accept List	1
LE Extended Create Connection [v1]	1
LE Remove Advertising Set	1
LE Remove Device From Filter Accept List	1
LE Set Extended Advertising Data	1

HCI Command	Count
LE Set Periodic Advertising Enable	1
LE Set Extended Scan Response Data	1
LE Set Data Length	1
LE Set Advertising Set Random Address	1
LE Set Extended Advertising Parameters [v1]	1
Set Connection Encryption	1
Authentication Requested	1
Reset	1
Vendor Command 0xfc17	1
Write Inquiry Scan Activity	1
LE Read Buffer Size [v2]	1
LE Read Suggested Default Data Length	1
Write Secure Connections Host Support	1
Write Simple Pairing Mode	1
LE Read Maximum Data Length	1
LE Read Resolving List Size	1
LE Read Filter Accept List Size	1
Read Local Supported Codecs	1
Set Min Encryption Key Size	1
Write Voice Setting	1
Read Buffer Size	1
LE Set Event Mask	1
LE Read Supported States	1
LE Read Local Supported Features	1
Read Local Supported Commands	1
Read Local Version Information	1
Write LE Host Supported	1
LE Read Maximum Advertising Data Length	1
LE Read Number of Supported Advertising Sets	1

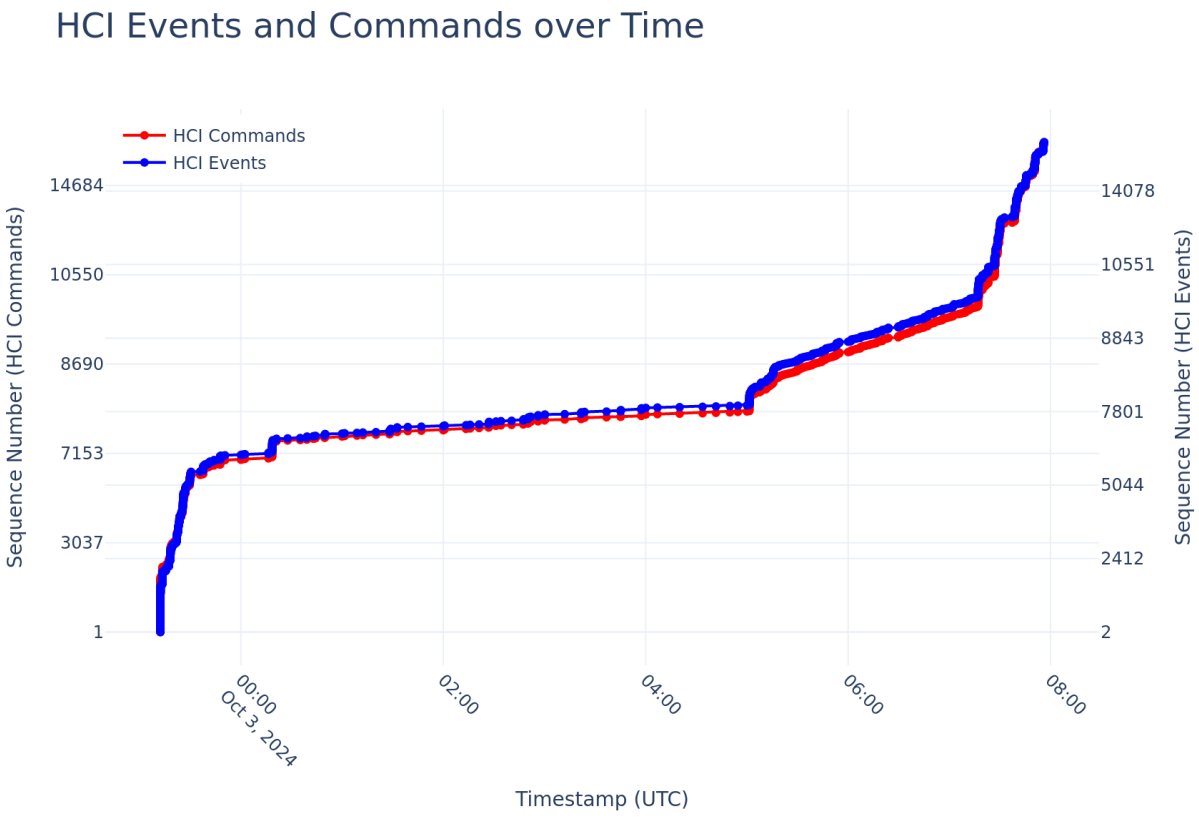
HCI Command	Count
LE Read Periodic Advertiser List Size	1
LE Set Host Feature	1
Set Event Mask	1
Change Local Name	1
Vendor Command 0xfd5e	1
LE Rand	1
Write Page Timeout	1
Write Class of Device	1
Write Inquiry Scan Type	1
Write Page Scan Type	1
Write Inquiry Mode	1
LE Set Resolvable Private Address Timeout	1
Read BD ADDR	1
Vendor Command 0xfd5f	1
Write Default Erroneous Data Reporting	1
Vendor Command 0xfd53	1
Read Default Erroneous Data Reporting	1
Accept Connection Request	1

HCI Event Counts:

HCI Event	Count
LE Meta	9733
Number of Completed Packets	1572
Command Complete	791
Command Status	307
Enhanced Flush Complete	58
Mode Change	40
Vendor-Specific	33
Connect Complete	5

HCI Event	Count
Read Remote Extended Features Complete	4
Read Remote Version Information Complete	3
Read Remote Supported Features	2
Max Slots Change	2
Connection Packet Type Changed	2
Link Key Request	2
Encryption Change	2
Read Clock Offset Complete	2
Disconnect Complete	1
Connect Request	1
Remote Name Request Complete	1
Authentication Complete	1
Role Change	1

The chart below/on the next page shows the variation of HCI commands and events over the timeframe of packet capture.



ACL Packet Summary

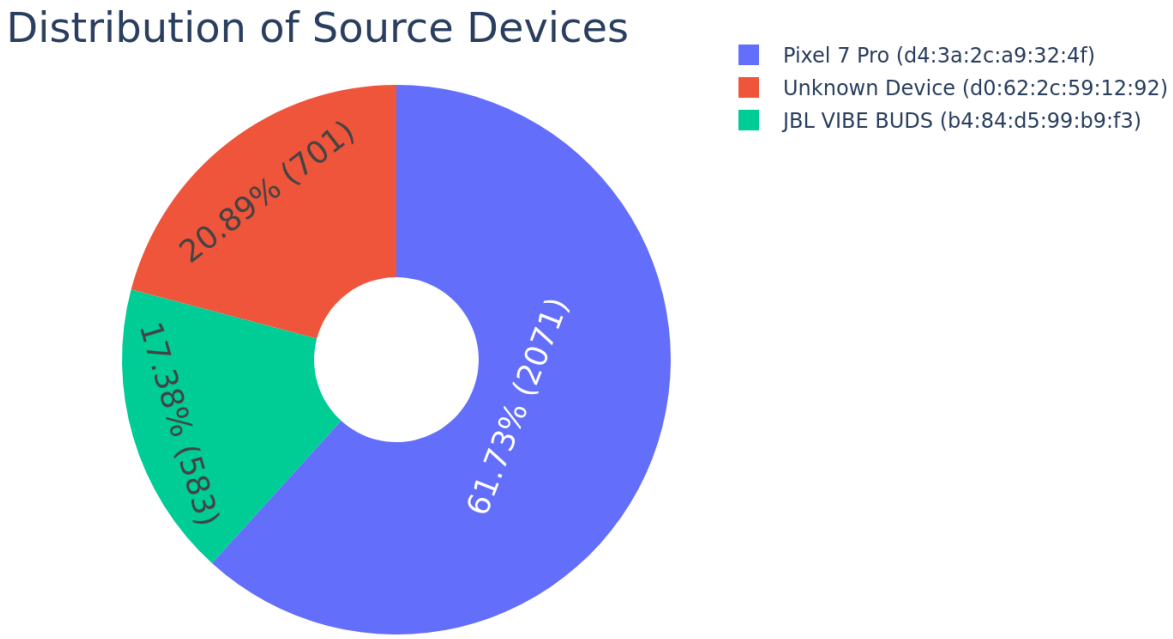
Bluetooth ACL, which is short for Bluetooth Asynchronous Connection-oriented Logical transport is used for general data transfer between the host and controller when it is not in real-time. It is provided alongside the SCO (Synchronous Connection Oriented) protocol which finds its use in audio and video data transfer in real-time.

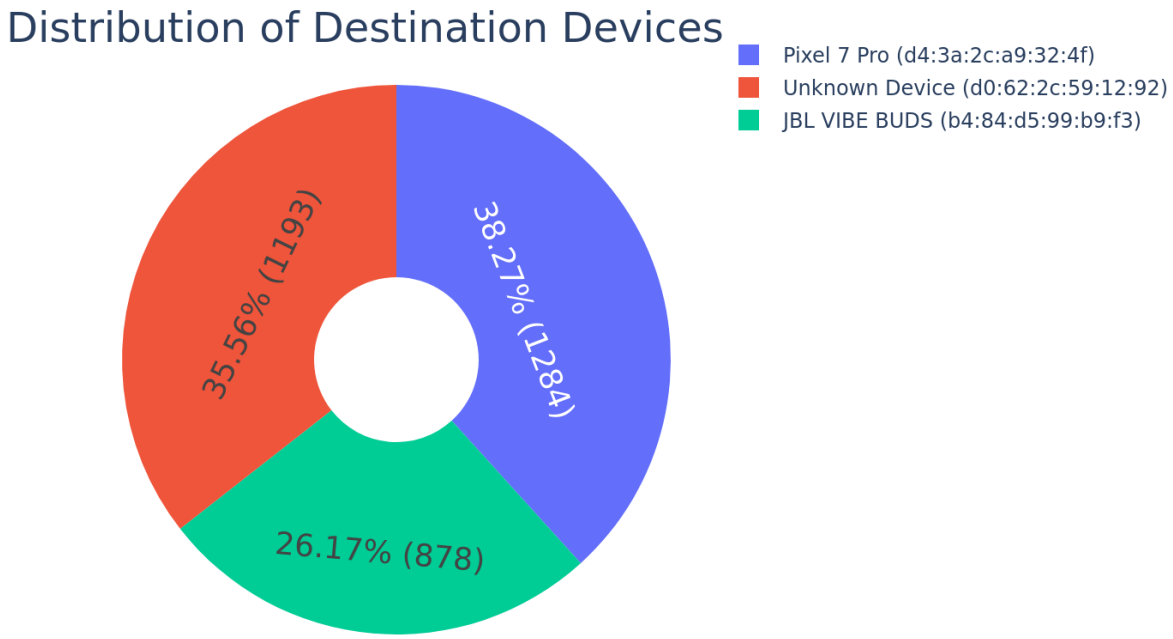
These packets usually have a higher chance of containing idetifying information about the devices in use such as the device name and mac addresses.

ACL LE Protocols Used: 8
Outgoing Data Packets: 2071
Incoming Data Packets: 1284

LE Protocol	Count
ACL - Attribute Protocol	1522
ACL - Audio/Video Distribution Transport Protocol	628
ACL - L2CAP Protocol	513
ACL - RFComm Hands Free Profile	348
ACL - Audio/Video Remote Control Profile	222
ACL - Radio Frequency Communication	58
ACL - Service Discovery Protocol	38
ACL - RFComm Data Transfer	26

The plots below depict the split up of packets to and from the host and the controllers it has connected to in the given timeframe.





From the MAC addresses in the ACL protocols, we can identify the device name and manufacturer information of the host and control devices in our capture files.

MAC Vendor Information

Host Device

Device Name: Pixel 7 Pro
MAC Address: d4:3a:2c:a9:32:4f
Manufacturer/Vendor: Google, Inc.
Address: 1600 Amphitheatre Parkway, Mountain View CA 94043, , US

Controller Devices

Controller 1

Device Name: JBL VIBE BUDS
MAC Address: b4:84:d5:99:b9:f3
Manufacturer/Vendor: GooWi Wireless Technology Co., Limited
Address: RM1601,Crative BuildingII East Tianan, City Futian Shenzhen Guangdong 518000, , CN

Controller 2

Device Name: Unknown Device
MAC Address: d0:62:2c:59:12:92
Manufacturer/Vendor: Xi'an Yipu Telecom Technology Co.,Ltd.
Address: Floor 5, Block C, Huanpu Industrial Park, 211 Tiangu 8th Road, Xi 'an Shaanxi 710076, , CN